CLAIMS

WE CLAIM:

1. A method of establishing a secure communication channel for information flow between two or more computers communicating via an interconnected computer network, comprising:

receiving a security association data structure from one or more computers via the interconnected computer network;

storing the received security association data structure in a memory region having a specific memory address associated therewith; and

assigning the specific memory address to a security parameter index value associated with the received security association data structure.

2. The method of Claim 1, further comprising:

transmitting the security parameter index value to the one or more computers from which the security association data structure was received.

3. The method of Claim 1, wherein the specific memory address and the security parameter index value, are both 32 bit values.

4. The method of Claim 1, wherein the received security association data structure is stored in a security association database that includes other security association data structures.

5. The method of Claim 1, wherein the received security association data structure comprises a network destination address value and a security protocol identifier.

6. A method of establishing a secure communication channel for information flow between two or more computers communicating via an interconnected computer network, comprising:

receiving a security association data structure from one or more computers via the interconnected computer network;

storing the received security association data structure in a memory region having a specific memory address associated therewith;

assigning the specific memory address to a security parameter index value; and

transmitting the security parameter index value to the one or more computers from which the security association data structure was received.

7. The method of Claim 6, wherein the specific memory address and the security parameter index value, are both 32 bit values.

8. The method of Claim 6, wherein the received security association data structure is stored in a security association database that includes other security association data structures.

9. A method of processing information received over a previously established secure communication channel, the method comprising:

receiving a data packet that includes at least an encrypted and/or authenticated data portion and one or more header portions, the one or more header portions including at least a security parameter index value;

locating a memory region using the security parameter index value as an address pointer; and

processing the encrypted and/or authenticated data portion of the received data packet based on a security association data structure stored in the located memory region.

10. The method of Claim 9, wherein the one or more header portions of the data packet and the security association data structure each further includes a network destination address value, and wherein the method further comprises:

prior to processing the encrypted and/or authenticated data portion, determining whether the network destination address value in the one or more header portions matches the network destination address value in the security association data structure stored in the located memory region.

11. The method of Claim 9, wherein the security parameter index value is a 32 bit value.

12. The method of Claim 9, wherein the located memory region is part of a security association database that includes other memory regions that store other security association data structures.

13. The method of Claim 9, wherein:

the security association data structure stored in the located memory address includes a security protocol identifier; and

the processing of the encrypted and/or authenticated data portion includes decrypting and/or authenticating the encrypted and/or authenticated data portion based on a security protocol that is identified by the security protocol identifier.

14. The method of Claim 13, wherein the one or more header portions of the received data packet further includes a security protocol identifier, and wherein the method further comprises:

prior to processing the encrypted and/or authenticated data portion, determining whether the security protocol identifier in the one or more header portions matches the security protocol identifier in the security association data structure stored in the located memory region.

15. A method of processing information received over a previously established secure communication channel, the method comprising:

receiving a data packet that includes at least an encrypted and/or authenticated data portion and a one or more header portions, the one or more header portions including at least a security parameter index value and a network destination address value;

locating a memory region using the security parameter index value as an address pointer;

determining whether the network destination address value in the header portion matches a network destination address of a security association data structure stored in the located memory region; and

in response to the determination that the network destination address values match, processing the encrypted and/or authenticated data portion of the received data packet based on the security association data structure stored in the located memory region.

16. The method of Claim 15, wherein the security parameter index value is a 32 bit value.

17. The method of Claim 15, wherein the located memory region is part of a security association database that includes other memory regions that store other security association data structures.

18. The method of Claim 15, wherein:

the security association data structure stored in the located memory address includes a security protocol identifier; and

the processing of the encrypted and/or authenticated data portion includes decrypting and/or authenticating the encrypted and/or authenticated data portion based on a security protocol that is identified using the security protocol identifier.

19. The method of Claim 18, wherein the one or more header portions of the received data packet further includes a security protocol identifier, and wherein the method further comprises:

prior to processing the encrypted and/or authenticated data portion, determining that the security protocol identifier in the one or more header portion matches the security protocol identifier in the security association data structure stored in the located memory region.

20. A method of processing information received over a previously established secure communication channel, the method comprising:

receiving a data packet that includes at least an encrypted and/or an authenticated data portion and one or more header portions, the one or more header portions including at least a security parameter index value, a network destination address value, and a security protocol identifier;

locating a memory region using the security parameter index value as an address pointer;

determining whether the network destination address value and the security protocol identifier in the one or more header portions each match a network destination address value and a security protocol identifier in a security association data structure stored in the located memory region; and

in response to the determination that the network destination addresses values and security protocol identifiers both match, processing the encrypted and/or authenticated data portion of the received data packet based on the security protocol in the security association data structure stored in the located memory region.

21. A method of determining an appropriate security association for an encrypted data packet received by a first computer over a previously established secure communication channel in an interconnected computer network, the method comprising:

parsing a security parameter index value from a header portion of the received data packet;

locating a memory region having an address that matches the security parameter index value; and

implementing a security association based on a security association data structure that is stored in the located memory region.

22. The method of Claim 21, wherein the header portion of the received data packet and the security association data structure each further include a network destination address value, and wherein the method further comprises:

prior to implementing the security association, determining that the network destination address value in the header portion matches the network destination address value in the security association data structure.

23. The method of Claim 21, wherein the security parameter index value is a 32 bit value.

24. The method of Claim 21, wherein the located memory region is part of a security association database that includes other memory regions that store other security association data structures.

25. The method of Claim 21, wherein the header portion of the received data packet and the security association data structure each further include a security protocol identifier, and wherein the method further comprises:

prior to implementing the security association, determining that the security protocol identifier in the header portion matches the security protocol identifier in the security association data structure stored in the located memory region.

26. The method of Claim 25, further comprising:

processing the received data packet based on the security protocol.

27. A method of determining an appropriate security association for an encrypted and/or authenticated data packet received by a first computer over a previously established secure communication channel in an interconnected computer network, the method comprising:

parsing a security parameter index value and a destination address value from a header portion of the received data packet;

locating a memory region having an address that matches the security parameter index value;

determining whether the network destination address value in the header portion matches a network destination address value in a security association data structure that is stored in the located memory address; and

in response to the determination that the network destination address values match, implementing a security association based on the security association data structure that is stored in the located memory region.

28. The method of Claim 27, wherein the security parameter index value is a 32 bit value.

29. The method of Claim 27, wherein the located memory region is part of a security association database that includes other security association data structures.

30. The method of Claim 27, wherein the header portion of the received data packet and the security association data structure each further include a security protocol identifier, and wherein the method further comprises:

prior to implementing the security association, determining that the security protocol identifier in the header portion matches the security protocol

identifier in the security association data structure stored in the located memory region.

31. The method of Claim 30, further comprising:

processing the received data packet based on the security protocol.

32. A method of determining an appropriate security association for an encrypted and/or authenticated data packet received by a first computer over a previously established secure communication channel in an interconnected computer network, the method comprising:

parsing a security parameter index value, a destination address value, and a security protocol identifier from a header portion of the received data packet;

locating a memory region having an address that matches the security parameter index value;

determining whether the network destination address value and the security protocol identifier in the header portion match a network destination address value and a security protocol identifier in a security association data structure that is stored in the located memory address; and

in response to the determination that the network destination address values and security protocol identifiers match, implementing a security association based on the security association data structure that is stored in the located memory region.

33. The method of Claim 32, wherein the security parameter index value is a 32 bit value.

34. The method of Claim 32, wherein the located memory region is part of a security association database that includes other security associations.

35. The method of Claim 32, further comprising:

processing the received data packet based on the security protocol.

36. A computer-readable medium containing computer executable code for instructing a computer to establish a secure communication channel for information flow between one or more other computers communicating via an interconnected computer network, the instructions comprising:

receiving a security association data structure from one or more computers via the interconnected computer network;

storing the received security association data structure in a memory region having a specific memory address associated therewith; and

assigning the specific memory address to a security parameter index value associated with the received security association data structure.

37. A computer-readable medium containing computer executable code for instructing a computer to process information received over a previously established secure communication channel, the instructions comprising:

receiving a data packet that includes at least an encrypted and/or authenticated data portion and a header portion, the header portion including at least a security parameter index value;

locating a memory region using the security parameter index value as an address pointer; and

processing the encrypted and/or authenticated data portion of the received data packet based on a security association data structure stored in the located memory region.